#5

대 한 민 국 특 허 청

KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : Application Number	특허출원 2001년 제 40684 호 PATENT-2001-0040684
출 원 년 월 일 : Date of Application	2001년 07월 07일 JUL 07, 2001
출 원 인 : Applicant(s)	삼성전자 주식회사 SAMSUNG ELECTRONICS CO., LTD.

2001 년 08 월 10 일

특 허 청

COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0003
【제출일자】	2001.07.07
【국제특허분류】	G06F
【발명의 명칭】	데이터베이스 내의 정보를 안전하게 관리하는 방법
【발명의 영문명칭】	Method to securely manage information in database
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	강춘운
【성명의 영문표기】	KANG,Chun Un
【주민등록번호】	730216-1031412
【우편번호】	122-110
【주소】	서울특별시 은평구 구파발동 75-15호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 이해영 (인)

【수수료】

【기본출원료】	16	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	8	항	365,000 원
【합계】	394,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명의 정보 관리 방법은, 데이터베이스에 복수의 중요 정보들을 저장하고 저장된 중요 정보들을 안전하게 관리하는 방법이다. 이 방법은 암호화, 저장 및 확인 단계들을 포함한다. 암호화 단계에서는, 중요 정보들중에서 적어도 한 중요 정보가 갱신될 때마다 변하는 동기화 정보가 중요 정보들과 함께 데이터베이스에 저장되고, 동기화 정보가 암호화된다. 저장 단계에서는, 암호화된 동기화 정보가 분산되어 소정의 장소들에 저장된다. 확인 단계에서는, 소정의 장소들에 저장된 동기화 정보가 조합 및 해독되어, 데이터베이스에 저장된 동기화 정보와 일치하는지 확인된다.

【대표도】

도 4

【색인어】

동기화 정보

【명세서】

【발명의 명칭】

데이터베이스 내의 정보를 안전하게 관리하는 방법{Method to securely manage information in database}

【도면의 간단한 설명】

도 1은 디지털 권리 운영을 위한 일반적인 통신망 시스템을 보여주는 도면이다.

도 2는 종래의 컨텐츠 파일의 구조를 보여주는 블록도이다.

도 3은 본 발명의 일 실시예에 의한 컨텐츠 파일의 구조를 보여주는 블록도이다.

도 4는 도 3의 컨텐츠 파일의 암호화된 동기화 정보가 분산되어 소정의 장소들에 저장되는 상태를 보여주는 도면이다.

도 5는 도 3의 컨텐츠 파일의 중요 정보인 디.알.엠 정보를 안전하게 관리하기 위하여 사용자 컴퓨터에 의하여 실행되는 프로그램의 일 예를 보여주는 흐름도이다.

도 6은 도 3의 컨텐츠 파일의 중요 정보인 디.알.엠 정보를 안전하게 관리하기 위하여 사용자 컴퓨터에 의하여 실행되는 프로그램의 다른 예를 보여주는 흐름도이다.

<도면의 주요 부분에 대한 부호의 설명>

10...사용자 컴퓨터, 12...통신망,

141...컨텐츠 제공 서버, 142...열쇠-데이터 운영 서버,

143...결제 시스템, SI1, SI2, SI3...분산 동기화 정보,

31, 41...헤더, 32, 42...컨텐츠 파일의 데이터,

EI...암호화 정보, KU...사용자 열쇠-데이터,

DRM...디.알.엠 정보, KS...동기화-정보 열쇠-데이터,

KD...디.알.엠-정보 열쇠-데이터, SI...동기화 정보.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<15> 본 발명은, 데이터베이스 내의 정보를 안전하게 관리하는 방법에 관한 것으로서, 보다 상세하게는, 데이터베이스에 복수의 중요 정보들을 저장하고 저장된 중요 정보들을 안전하게 관리하는 방법에 관한 것이다.

<16> 도 1은 디지털 권리 운영(DRM, Digital Right Management)을 위한 일반적인 통신망 시스템 예를 들어, 인터넷 시스템을 보여주는 도면이다. 도 1을 참조하면, 사용자 컴퓨터들(10), 컨텐츠 제공 서버(141), 열쇠-데이터 운영 서버(142) 및 결제 시스템(143)이 통신망(12)을 통하여 서로 연결된다. 컨텐츠 제공 서버(141)는 사용자 컴퓨터들(10)에 컨텐츠를 제공하면서 디지털 권리 운영(DRM)과 관련한 사용 요금을 결제 시스템(143)을 통하여 받는다. 열쇠-데이터 운영 서버(142)는 컨텐츠 제공 서버(141)로부터 사용자 컴퓨터들(10)에 제공된 컨텐츠 파일의 암호화 및 해독하기 위한 열쇠-데이터를 운영한다.

<17> 도 2를 참조하면, 종래의 컨텐츠 파일은 헤더(31)와 컨텐츠 파일의 데이터(32)를 포함한다. 헤더(31)는 암호화 정보(EI), 사용자 열쇠-데이터(KU) 및 디.알.엠 정보(DRM)를 포함한다. 암호화 정보(EI)는 컨텐츠 파일의 데이터(32)를 암호화하는 데에 사용되는 파라메터 등의 정보이다. 사용자 열쇠-데이터(KU)는 컨텐츠 파일의 데이터(32)의 암호화 및 해독에 사용되는 열쇠-데이터이다. 디.알.엠 정보(DRM)는 사용자의 사용 가능 횟수의 정보이다.

<18> 위와 같은 종래의 파일 구조에 따른 단순한 정보 관리 방법에 의하면, 헤더(31) 자체가 난해하게 암호화된다 하더라도 해커(hacker)에 의하여 헤더(31)가 해독될 수 있다. 이와 같은 경우, 해커는 중요 정보 예를 들어, 디.알.엠 정보(DRM)를 변경할 수 있다. 따라서, 데이터베이스 내의 정보를 보다 안전하게 관리하려면, 정보의 암호화와 더불어, 암호화된 정보가 해킹된 적이 있는지의 여부를 효율적으로 확인할 필요가 있다.

【발명이 이루고자 하는 기술적 과제】

<19> 본 발명의 목적은, 정보의 암호화와 더불어, 암호화된 정보가 해킹된 적이 있는지의 여부를 효율적으로 확인함에 따라, 암호화 자체에만 의존하지 않고서도 데이터베이스 내의 정보를 보다 안전하게 관리하는 방법을 제공하는 것이다.

【발명의 구성 및 작용】

<20> 상기 목적을 이루기 위한 본 발명의 정보 관리 방법은, 데이터베이스에 복수의 중요 정보들을 저장하고 저장된 중요 정보들을 안전하게 관리하는 방법이다. 이 방법은 암호화, 저장 및 확인 단계들을 포함한다. 상기 암호화 단

계에서는, 상기 중요 정보들중에서 적어도 한 중요 정보가 갱신될 때마다 변하는 동기화 정보가 상기 중요 정보들과 함께 상기 데이터베이스에 저장되고, 상기 동기화 정보가 암호화된다. 상기 저장 단계에서는, 상기 암호화된 동기화 정보가 분산되어 소정의 장소들에 저장된다. 상기 확인 단계에서는, 상기 소정의 장소들에 저장된 동기화 정보가 조합 및 해독되어, 상기 데이터베이스에 저장된 동기화 정보와 일치하는지 확인된다.

<21> 본 발명의 상기 정보 관리 방법에 의하면, 상기 소정의 장소들에 저장된 동기화 정보가 조합 및 해독되어, 상기 데이터베이스에 저장된 동기화 정보와 일치하는지 확인된다. 이에 따라, 상기 중요 정보가 해킹된 적이 있는지의 여부가 효율적으로 확인될 수 있음에 따라, 암호화 자체에만 의존하지 않고서도 데이터베이스 내의 정보를 보다 안전하게 관리할 수 있다. 또한, 상기 암호화된 동기화 정보가 분산되어 소정의 장소들에 저장되므로, 상기 암호화된 동기화 정보가 노출될 위험성이 최소화된다.

<22> 이하, 본 발명에 따른 바람직한 실시예가 상세히 설명된다.

<23> 도 3은 본 발명의 일 실시예에 의한 컨텐츠 파일의 구조를 보여준다. 도 3을 참조하면, 본 발명에 따른 컨텐츠 파일은 헤더(41)와 컨텐츠 파일의 데이터(42)를 포함한다. 헤더(41)는 암호화 정보(EI), 사용자 열쇠-데이터(KU), 동기화-정보 열쇠-데이터(KS), 디.알.엠-정보 열쇠-데이터(KD), 동기화 정보(SI) 및 중요 정보로서의 디.알.엠 정보(DRM)를 포함한다.

<24> 암호화 정보(EI)는 컨텐츠 파일의 데이터(42)를 암호화하는 데에 사용되는

파라메터 등의 정보이다. 사용자 열쇠-데이터(KU)는 컨텐츠 파일의 데이터(42)의 암호화 및 해독에 사용되는 열쇠-데이터이다. 동기화-정보 열쇠-데이터(KS)는 동기화 정보(SI)의 암호화 및 해독에 사용되는 열쇠-데이터이다. 디.알.엠-정보 열쇠-데이터(KD)는 디.알.엠 정보(DRM)의 암호화 및 해독에 사용되는 열쇠-데이터이다. 동기화 정보(SI)는 중요 정보로서의 디.알.엠 정보(DRM)가 해킹되었는지의 여부를 확인하기 위하여 지속적으로 갱신되는 정보이다. 이 동기화 정보(SI)는 디.알.엠 정보(DRM)에 내장될 수도 있다. 중요 정보로서의 디.알.엠 정보(DRM)는 사용자의 사용 가능 횟수의 정보이다.

<25> 도 4를 참조하면, 도 3의 컨텐츠 파일의 암호화된 동기화 정보(SI)는 분산되어 소정의 장소들에 저장되는 상태를 보여준다. 예를 들어, 사용자 컴퓨터(도 1의 10) 자체에서만 본 발명에 따른 정보 관리 방법이 적용되는 경우(이 경우에는 중요 정보가 디.알.엠 정보(도 3의 DRM)가 아닐 것이다), 암호화된 동기화 정보(SI)는 분산되어 하드 디스크의 소정의 장소들에 저장된다. 한편, 도 1에 도시된 바와 같은 통신망 시스템의 경우, 암호화된 동기화 정보(SI)는 분산되어 열쇠-데이터 운영 서버(142)에 저장될 수 있다. 이와 같이, 암호화된 동기화 정보(SI)가 분산되어 소정의 장소들에 저장되므로, 암호화된 동기화 정보가 노출될 위험성이 최소화된다. 이와 같은 원리에 의하여, 동기화 정보(도 3의 SI) 및 동기화-정보 열쇠-데이터(도 3의 KS)가 소정의 장소들에 분산되어 저장된다(도 5의 프로그램의 경우). 이와 더불어, 중요 정보로서의 디.알.엠 정보(DRM) 및 디.알.엠-정보 열쇠-데이터(KD)도 소정의 장소들에 분산되어 저장될 수 있다(도 6의 프로그램의 경우).

<26> 도 5는 도 3의 컨텐츠 파일의 중요 정보인 디.알.엠 정보(DRM)를 안전하게 관리하기 위하여 사용자 컴퓨터(도 1의 10)에 의하여 실행되는 프로그램의 일 예를 보여준다. 도 5의 프로그램은, 중요 정보로서의 디.알.엠 정보(도 3의 DRM)가 암호화되지 않는 경우이므로, 디.알.엠-정보 열쇠-데이터(도 3의 KD)가 필요하지 않는다. 도 5의 프로그램을 순서대로 설명하면 다음과 같다.

<27> 먼저, 소정의 장소들에 분산되어 저장된 동기화-정보 열쇠-데이터가 조합 및 해독된다(단계 S501). 다음에, 소정의 장소들에 분산되어 저장된 동기화-정보가 조합 및 해독된다(단계 S502). 단계 S502의 해독 단계에서는, 단계 S501에서 해독된 동기화-정보 열쇠-데이터에 의하여 동기화-정보가 해독된다. 다음에, 데이터베이스 예를 들어, 사용자 컴퓨터(도 1의 10) 내의 하드디스크에 암호화되어 저장된 동기화 정보(도 3의 SI)가 해독된다(단계 S503). 다음에, 단계 S502 및 S503에서 해독된 동기화 정보들이 서로 일치하는지 확인된다(단계 S504). 일치하지 않는 경우, 디.알.엠 정보(도 3의 DRM)를 포함한 컨텐츠 파일이 해킹되었음을 의미한다. 따라서, 해킹 정보가 표시되고(단계 S506) 해킹 정보가 서버 예를 들어, 컨텐츠 제공 서버(도 1의 141) 및/또는 열쇠-데이터 운영 서버(도 1의 142)에 전송된다(단계 S507).

<28> 단계 S502 및 S503에서 해독된 동기화 정보들이 서로 일치하면(단계 S504), 중요 정보로서의 디.알.엠 정보(DRM)의 갱신이 모니터링된다(단계 S508). 이와 같은 디.알.엠 정보(DRM)의 갱신은 예를 들어, 컨텐츠 파일의 데이터(도 3의 42)의 사용 횟수와 관련이 있다. 디.알.엠 정보(DRM)가 갱신되면, 새로운 동기화 정보 및 중요 정보로서의 디.알.엠 정보(DRM)가 데이터베이스에 저장된다(단계

S509). 다음에, 데이터베이스에 저장된 동기화 정보(도 3의 SI)가 암호화된다(단계 S510). 또한, 암호화된 동기화 정보(SI)의 열쇠-데이터(도 3의 KS)가 암호화된다(단계 S511). 다음에, 암호화된 동기화 정보 및 그 열쇠 데이터가 소정의 장소들에 분산되어 저장된다(단계 S512). 상기 단계 S508 내지 S512는 종료 신호가 입력될 때까지 반복 수행된다(단계 S513).

<29> 도 6은 도 3의 컨텐츠 파일의 중요 정보인 디.알.엠 정보(DRM)를 안전하게 관리하기 위하여 사용자 컴퓨터(도 1의 10)에 의하여 실행되는 프로그램의 다른 예를 보여준다. 도 6의 프로그램은, 중요 정보로서의 디.알.엠 정보(도 3의 DRM)도 암호화되는 경우이므로, 디.알.엠-정보 열쇠-데이터(도 3의 KD)가 사용된다. 도 6의 프로그램을 순서대로 설명하면 다음과 같다.

<30> 먼저, 소정의 장소들에 분산되어 저장된 동기화-정보 및 중요 정보로서의 디.알.엠 정보의 열쇠-데이터들이 조합 및 해독된다(단계 S601). 다음에, 소정의 장소들에 분산되어 저장된 동기화-정보 및 중요 정보로서의 디.알.엠 정보가 조합 및 해독된다(단계 S602). 단계 S602의 해독 단계에서는, 단계 S601에서 해독된 동기화-정보 및 및 디.알.엠 정보의 열쇠-데이터들에 의하여 동기화-정보 및 디.알.엠 정보가 해독된다. 다음에, 데이터베이스 예를 들어, 사용자 컴퓨터(도 1의 10) 내의 하드디스크에 암호화되어 저장된 동기화 정보(도 3의 SI) 및 중요 정보로서의 디.알.엠 정보(도 3의 DRM)가 해독된다(단계 S603). 다음에, 단계 S602 및 S603에서 해독된 동기화 정보들 및 중요 정보들(디.알.엠 정보들)이 각각 일치하는지 확

인된다(단계 S604). 일치하지 않는 경우, 디.알.엠 정보(도 3의 DRM)를 포함한 컨텐츠 파일이 해킹되었음을 의미한다. 따라서, 해킹 정보가 표시되고(단계 S606) 해킹 정보가 서버 예를 들어, 컨텐츠 제공 서버(도 1의 141) 및/또는 열쇠-데이터 운영 서버(도 1의 142)에 전송된다(단계 S607).

<31> 단계 S602 및 S603에서 해독된 동기화 정보들 및 중요 정보들(디.알.엠 정보들)이 각각 일치하면(단계 S604), 중요 정보로서의 디.알.엠 정보(DRM)의 갱신이 모니터링된다(단계 S608). 이와 같은 디.알.엠 정보(DRM)의 갱신은 예를 들어, 컨텐츠 파일의 데이터(도 3의 42)의 사용 횟수와 관련이 있다. 디.알.엠 정보(DRM)가 갱신되면, 새로운 동기화 정보 및 중요 정보로서의 디.알.엠 정보(DRM)가 데이터베이스에 저장된다(단계 S609). 다음에, 데이터베이스에 저장된 동기화 정보(도 3의 SI) 및 중요 정보로서의 디.알.엠 정보(DRM)가 암호화된다(단계 S610). 또한, 암호화된 동기화 정보(SI) 및 중요 정보로서의 디.알.엠 정보(DRM)의 열쇠-데이터들(도 3의 KS, KD)이 암호화된다(단계 S611). 다음에, 암호화된 동기화 정보, 중요 정보로서의 디.알.엠 정보 및 그 열쇠 데이터들이 소정의 장소들에 분산되어 저장된다(단계 S612). 상기 단계 S608 내지 S612는 종료 신호가 입력될 때까지 반복 수행된다(단계 S613).

【발명의 효과】

<32> 이상 설명된 바와 같이, 본 발명에 따른 정보 관리 방법에 의하면, 주기적으로 소정의 장소들에 저장된 동기화 정보가 조합 및 해독되어, 데이터베이스에 저장된 동기화 정보와 일치하는지 확인된다. 이에 따라, 중요 정보가 해킹된 적이 있는

지의 여부가 효율적으로 확인될 수 있음에 따라, 암호화 자체에만 의존하지 않고서도 데이터베이스 내의 정보를 보다 안전하게 관리할 수 있다. 또한, 암호화된 동기화 정보가 분산되어 소정의 장소들에 저장되므로, 암호화된 동기화 정보가 노출될 위험성이 최소화된다.

<33> 본 발명은, 상기 실시예에 한정되지 않고, 청구범위에서 정의된 발명의 사상 및 범위 내에서 당업자에 의하여 변형 및 개량될 수 있다.

【특허청구범위】

【청구항 1】

데이터베이스에 복수의 중요 정보들을 저장하고 저장된 중요 정보들을 안전하게 관리하는 방법에 있어서,

상기 중요 정보들중에서 적어도 한 중요 정보가 갱신될 때마다 변하는 동기화 정보를 상기 중요 정보들과 함께 상기 데이터베이스에 저장하고, 상기 동기화 정보를 암호화하는 단계;

상기 암호화된 동기화 정보를 분산하여 소정의 장소들에 저장하는 단계; 및

상기 소정의 장소들에 저장된 동기화 정보를 조합 및 해독하여, 상기 데이터베이스에 저장된 동기화 정보와 일치하는지를 확인하는 단계를 포함한 정보 관리 방법.

【청구항 2】

제1항에 있어서, 상기 암호화하는 단계에서,

상기 동기화 정보를 암호화 및 해독하기 위한 열쇠-데이터가 암호화되는 정보 관리 방법.

【청구항 3】

제2항에 있어서, 상기 저장하는 단계에서,

상기 암호화된 열쇠-데이터가 분산되어 소정의 장소들에 저장되는 정보 관리 방법.

【청구항 4】

제1항에 있어서, 상기 암호화하는 단계에서,

상기 갱신된 중요 정보가 암호화되는 정보 관리 방법.

【청구항 5】

제4항에 있어서, 상기 저장하는 단계에서,

상기 암호화된 중요 정보가 분산되어 소정의 장소들에 저장되는 정보 관리 방법.

【청구항 6】

제5에 있어서, 상기 확인하는 단계에서,

상기 소정의 장소들에 저장된 중요 정보가 조합 및 해독되어, 상기 데이터베이스에 저장된 중요 정보와 일치하는지 확인되는 정보 관리 방법.

【청구항 7】

제4항에 있어서, 상기 암호화하는 단계에서,

상기 중요 정보를 암호화 및 해독하기 위한 열쇠-데이터가 암호화되는 정보 관리 방법.

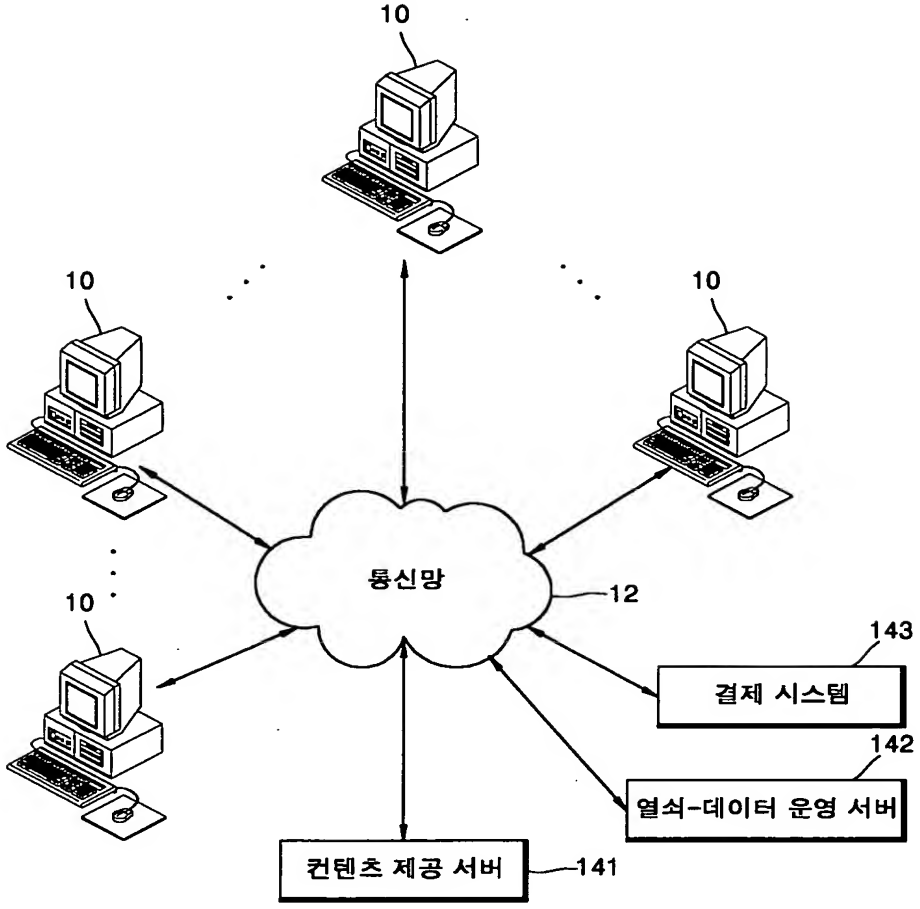
【청구항 8】

제7항에 있어서, 상기 저장하는 단계에서,

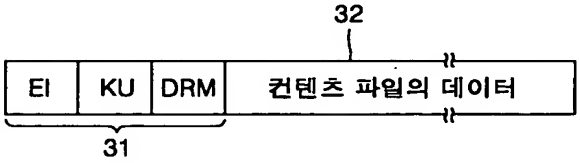
상기 암호화된 열쇠-데이터가 분산되어 소정의 장소들에 저장되는 정보 관리 방법.

【도면】

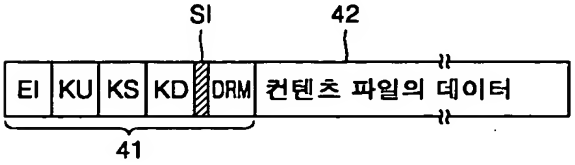
【도 1】


10
10
10
10
통신망
12
143
결제 시스템
142
열쇠-데이터 운영 서버
컨텐츠 제공 서버
141

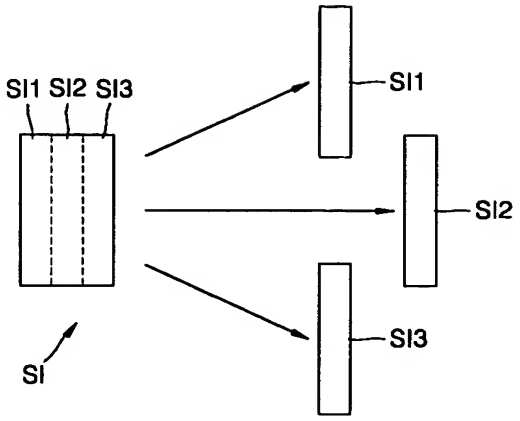
【도 2】


32
EI
KU
DRM
컨텐츠 파일의 데이터
31

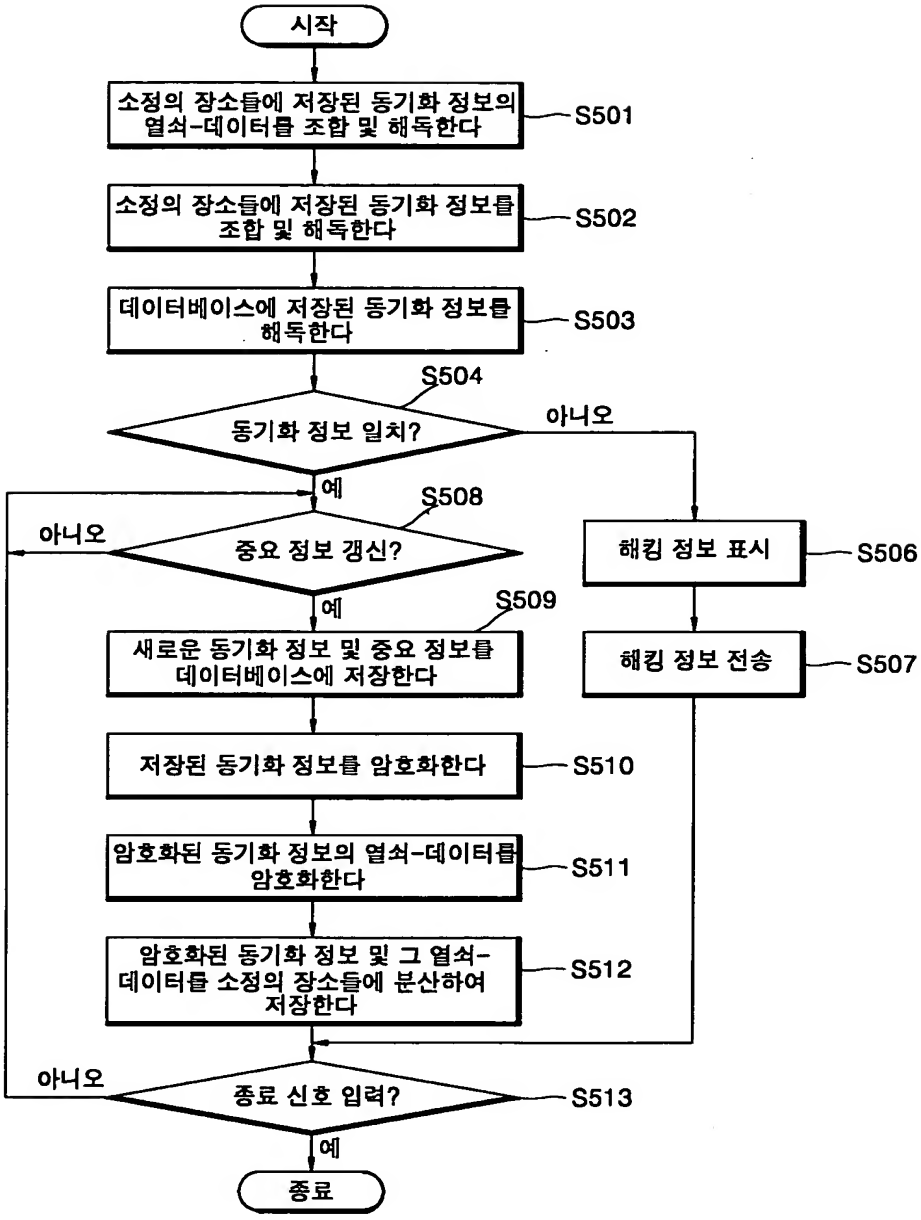
【도 3】


SI
42
EI
KU
KS
KD
DRM
컨텐츠 파일의 데이터
41

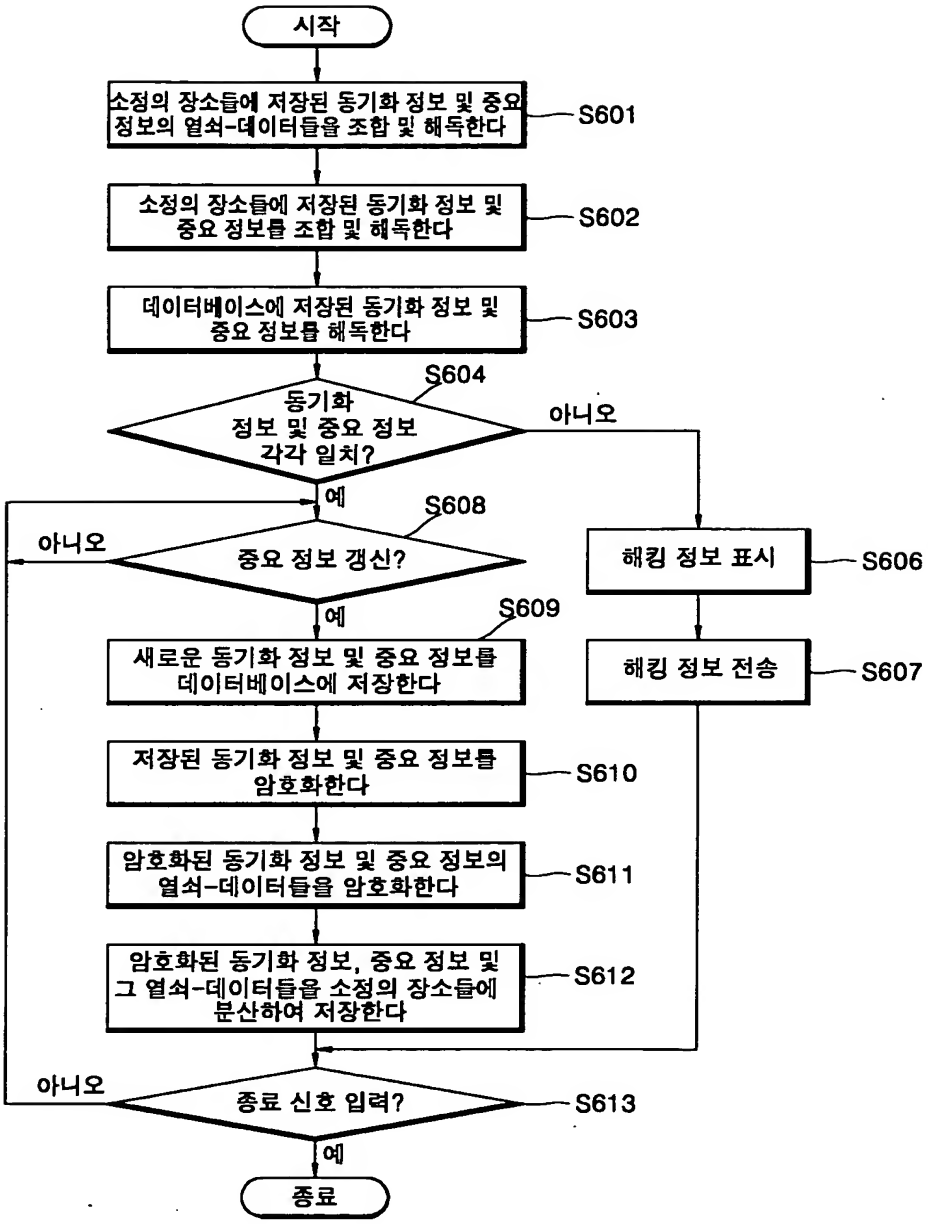
【도 4】



【도 5】


시작
소정의 장소들에 저장된 동기화 정보의 열쇠-데이터를 조합 및 해독한다
S501
소정의 장소들에 저장된 동기화 정보를 조합 및 해독한다
S502
데이터베이스에 저장된 동기화 정보를 해독한다
S503
S504
동기화 정보 일치?
아니오
예
S508
중요 정보 갱신?
아니오
예
해킹 정보 표시
S506
S509
새로운 동기화 정보 및 중요 정보를 데이터베이스에 저장한다
해킹 정보 전송
S507
저장된 동기화 정보를 암호화한다
S510
암호화된 동기화 정보의 열쇠-데이터를 암호화한다
S511
암호화된 동기화 정보 및 그 열쇠-데이터를 소정의 장소들에 분산하여 저장한다
S512
아니오
종료 신호 입력?
S513
예
종료

【도 6】


시작
소정의 장소들에 저장된 동기화 정보 및 중요 정보의 열쇠-데이터들을 조합 및 해독한다
S601
소정의 장소들에 저장된 동기화 정보 및 중요 정보를 조합 및 해독한다
S602
데이터베이스에 저장된 동기화 정보 및 중요 정보를 해독한다
S603
S604
동기화 정보 및 중요 정보 각각 일치?
아니오
예
S608
중요 정보 갱신?
아니오
예
해킹 정보 표시
S606
S609
새로운 동기화 정보 및 중요 정보를 데이터베이스에 저장한다
해킹 정보 전송
S607
저장된 동기화 정보 및 중요 정보를 암호화한다
S610
암호화된 동기화 정보 및 중요 정보의 열쇠-데이터들을 암호화한다
S611
암호화된 동기화 정보, 중요 정보 및 그 열쇠-데이터들을 소정의 장소들에 분산하여 저장한다
S612
아니오
종료 신호 입력?
S613
예
종료